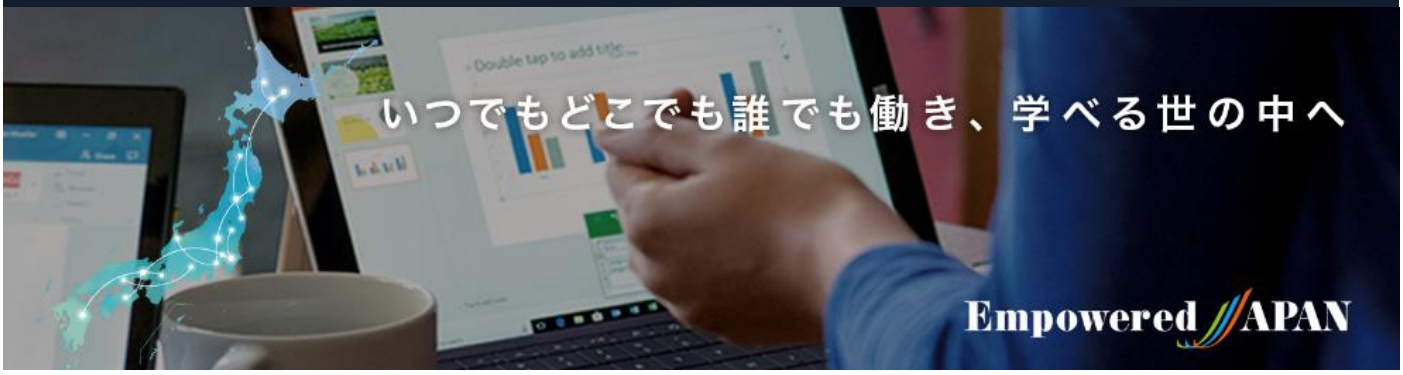
Empowered JAPAN 実行委員会 緊急ウェブセミナー 講演レポート



Empowered JAPAN 緊急ウェブセミナー

Empowered JAPAN 実行委員会はテレワークをはじめとする働き方改革や学び直しを通した「いつでもどこでも誰でも、働き、学べる世の中へ」をコンセプトに、2018 年に発足しました。東京圏および地方都市におけるテレワーク啓蒙イベントをはじめ、多くの自治体や協力会社と共に企業・個人向けテレワーク研修を実施してきました。この度のコロナウイルス感染拡大と 2020 年 2 月 25 日の政府基本方針に含まれた「テレワーク推奨」の呼びかけを受け、全国の組織や個人がテレワークを早期に実施するため、実践的な情報をお伝えするための緊急ウェブセミナーを 2020 年 3 月 17 日より連続的に無料開催しています。

カテゴリ：

IT ツール、環境

開催日時：2020 年 3 月 31 日

講師：

トレンドマイクロ株式会社
ビジネスマーケティング本部エンタープライズソリューション部　シニアマネージャ
吉田 睦氏

国内大手 SI を皮切りに、ハイエンド Unix サーバでのプロダクトマネージャや企業向けミッドレンジストレージの OEM 提供など外資系ベンダーにて日本向けに システムインフラを広める製品エキスパートとして活躍。トレンドマイクロへ入社以降 10 年以上に渡り、ゲートウェイ・セキュリテイ系一筋に 製品責任者として、またオンプレミスのみならずクラウド型セキュリティの立ち上げにも従事。

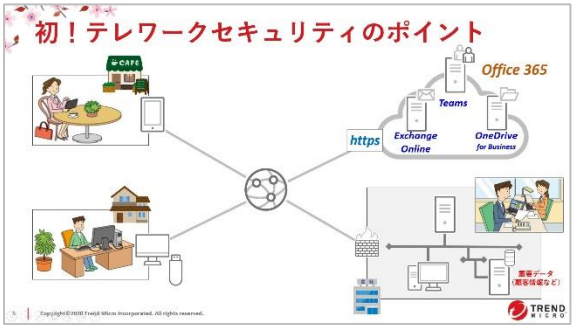
これから始めるテレワーク

～気になるセキュリティの第一歩～

テレワーク推進を阻む要因の一つが、「セキュリティ」の問題です。在宅勤務や社外のカフェなどでのリモートワークでは、情報漏洩を懸念して、ゆえに「テレワークの本格導入に踏み切れない」という声は頻繁に聞かれます。

これからテレワーク導入を検討する企業が、安全に業務を遂行するために気をつけるべきポイントはどこにあるのでしょうか。その"勘所"について解説してくださったのは、トレンドマイクロ株式会社ビジネスマーケティング部シニアマネージャの吉田睦氏です。吉田氏は、IT インフラの製品エキスパートとしての経験を長く積み、セキュリティ対策の普及啓発にも熱心に取り組まれています。

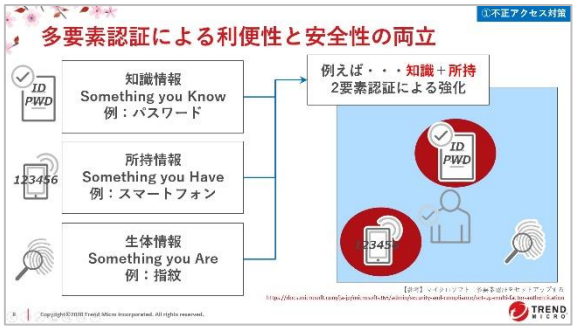
「テレワークにおけるセキュリティ面の外部からのリスクは大きく分けて 3 つ。不正なアクセス、盗難・紛失・覗き見、マルウェア（ウイルス）感染に分類されます。管理者は、これら 3 つのリスクのそれぞれに対応する策を講じる必要があります」（吉田氏）



まず、外部からの不正なアクセスを防ぐための大原則は「ID やパスワード管理の徹底」です。「『忘れないように』とパスワードを書いた付箋をパソコン本体に貼る方が時々いらっしゃいますが、これは玄関の鍵をドア前に置いておくのと同じ行為。パスワードもできるだけ推測しづらい数や文字の組み合わせにしましょう」（吉田氏）。

Empowered JAPAN 実行委員会 緊急ウェブセミナー 講演レポート

あらゆる手を尽くして不正アクセスを試みようとする侵入者に対抗するには、「ID とパスワードによる鍵かけだけでは不十分」と吉田氏は指摘。最近は、知識情報（パスワード、生年月日など）・所持情報（スマートフォンなど）・生体情報（指紋など）から異なる要素でのチェックを組み合わせた"多要素認証"を、特に外部からのアクセスでは採用すべきと説明します。「例えば、パスワードを入力（知識情報）した後に、更に生年月日の入力をするのは、多要素ではなく知識情報のみの多段階認証であり、より強固にするためにはパスワード入力後に、所持情報にあたる本人所有のスマートフォンに送られてきた番号入力を求めるなど"多要素での認証確認"がテレワーク時代には必須になる」（吉田氏）。



次に、マルウェア感染対策のポイントはどこにあるのでしょうか。マルウェアの感染経路は主に「USB」「ウェブ」「メール」。悪質な場合は瞬時に端末がロックされ、業務がストップしてしまうだけでなく、重要な情報を窃取されるリスクもあります。
感染を防ぐための第一歩は、OS・アプリ・ブラウザを最新にアップデートしておくことと、マルウェア対策ソフトを入れること。「メーカーが最新版をリリースする度に自動アップデートされる設定にするのがおすすめです」（吉田氏）。

加えて、感染経路別の対策として、「USB はウイルス対策に対応した製品のみを会社支給する」「業務に不要なアプリのインストールを禁止する」「利用していいクラウドサービスの認定と、クラウドに保存していいデータの種別ルール化」といった注意も必要に。
吉田氏によるとウェブ経由の感染で厄介なのは「ドライブ・バイ・ダウン」。これは、正規 Web サイトの脆弱性を狙った攻撃で、ユーザーが閲覧しているだけで不正プログラムが自動インストールされてしまうとのことです。この対策技術の選択にもポイントあり、ウェブサイトを種類別に選別する「フィルター機能」と、ウェブサイトの危険度を得点化して選別する「レピュテーション機能」の両方を組み合わせることで、「安全でふさわしいサイトのみ閲覧できる職場環境」が実現するのです。
また、攻撃者が侵入手口に使う「メール」は 9 割以上を占めており（2019 年同社調べ）、対策技術としてはサンドボックスなど高度な技術を採用すべき箇所であり、またテレワーカー側でも"なりすましメール"の手法を予防知識として持つことが重要に。「最近は、日本語の文面もこなれて、一見すると不正なメールとは気づきにくい。マウスを当てて送信者のメールアドレスを確認するなど、ちょっとした注意の意識を持つことが大切です」（吉田氏）。

最後に、盗難・紛失・覗き見対策となるアドバイスです。「社外で使うものだからこそ、万が一の紛失や盗難には備えて、HDD（ハードディスク）の暗号化はしておく。また、覗き見防止のためにプライバシースクリーンもぜひ採用を」と吉田氏は呼びかけます。もしもの事故発生時に追跡できるように、「監査ログ」の設定はオンにしておきましょう。

以上のような管理者側が備えるルールに実効性を持たせるには、それを使うワーカー側の「遵守」の意識付けが不可欠です。
在宅勤務においては、自宅 Wi-Fi（ルータ）を使用するケースも少なくありませんが、「安全性を高めるため、ID とパスワードは初期値から必ず変更を」（吉田氏）。外出時のネットワーク接続時には、会社から貸与されるモバイルルータの利用を原則とし、それができない場合には信用度の高い公衆 Wi-Fi を選ぶようにします。また、自動接続は「しない」設定にし、「重要な機密情報の送信は外出時には避ける」と決めておくなど、ワーカー側の行動モデルを示していくことも重要。日々変わるセキュリティ対策についてより詳しく知りたい場合は、最新情報を集めたサイト「iS702」も役立ちます。

「セキュリティを確定する要素は、ルール・人・技術。これら 3 つの歯車がうまく噛み合うことで、より強靭な安全性を実現できます」と吉田氏。歯車をスピーディーに動かしていくための経営者の理解・参画が求められています。